УДК 343.985.7

Я. А. Климова
профессор кафедры криминалистики
учебно-научного комплекса по предварительному следствию
в органах внутренних дел Волгоградской академии МВД России,
кандидат юридических наук

СПЕЦИФИКА РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Современный уровень развития различных IT-технологий и их повсеместное распространение в информационном пространстве способствовали появлению новых способов совершения преступлений.

Согласно статистическим данным, в 2020 году правоохранительные органы Российской Федерации зарегистрировали 510 400 преступлений, совершенных с помощью информационных технологий. В 2021 году на деяния рассматриваемой категории пришлось каждое четвертое из зарегистрированных преступлений (517 700 преступлений). В 2022 году зарегистрировано 522 100 преступлений, совершенных с помощью информационных технологий. В 2023 году с использованием информационно-телекоммуникационных технологий совершено каждое третье преступление (на 29,2 % преступлений больше, чем в 2022 году) [1; 2].

Согласимся с мнением В. В. Полякова, который полагает, что такое отставание вызвано неразработанностью частной криминалистической методики расследования высокотехнологичных преступлений [3, с. 85].

Кроме этого, проблемы расследования преступлений в условиях информационно-технологического развития общества рассматриваются в работах таких ученых-криминалистов, как А. А. Бессонов, В. Б. Вехов, Е. П. Ищенко, П. С. Пастухов, Е. Р. Россинская и др. [4; 5; 6; 7].

Следует подчеркнуть, что перечень преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, весьма значителен, и прогнозы по дальнейшей информатизации общества свидетельствуют о том, что он будет расширяться.

В последнее время все более популярным становится такой вид преступления, совершенного с использованием искусственного интеллекта, как мошенничество с применением технологии Deepfake.

Дипфéйк (англ. Deepfake, от deep learning — глубокое обучение и fake — подделка) — технология на базе искусственного интеллекта, позволяющая создавать ложные изображения и видео на основе реальных кадров [8].

Алгоритм анализирует большое количество снимков, видео и учится тому, как может выглядеть, говорить и двигаться конкретный человек. Нейросеть собирает из Интернета, в том числе из открытых источников в социальных сетях, фотографии человека с разными выражениями лица и создает из них новое изображение или видео.

Таким образом, нейросети научились создавать цифрового двойника практически любого человека. Они могут подделывать не только внешность, но и голос. Как только технология стала доступна всем, ее начали использовать и мошенники.

Поскольку генеральная идея любых дипфейков — максимальная реалистичность и правдоподобность, то уже сегодня можно наблюдать лавинообразный рост модифицированного контента, созданного с целью манипуляции сознанием отдельно взятого человека. Один из самых распространенных и при этом легких дипфейк-способов изъятия денежных средств у населения — запись мошенниками голоса жертвы (главная задача состоит в том, чтобы добиться произнесения ключевых слов, например, таких как «да»), на основе которой генерируется типовая звуковая дорожка для «общения» с роботом службы поддержки банка. Грамотно синтезированная на базе ключевых фрагментов запись позволяет «достоверно» ответить на все вопросы робота для перевода средств на нужный мошенникам счет.

В начале 2024 года уже зафиксированы попытки использования нового способа мошенничества в России: преступники, используя технологию дипфейка для подтверждения по видеозвонку личности владельца аккаунта, обращаются в банк с просьбой привязать личный кабинет к новому номеру телефона. После указанных действий мошенники получают полный доступ к личному кабинету потерпевшего и ко всем денежным средствам. При этом выявить подделку можно только с помощью специальных программ.

Так, в конце 2023 года СБЕР запатентовал технологию по распознаванию дипфейков, целью которой является повышение точности и эффективности обнаружения синтетического изменения изображений лиц людей в видео.

Основу технологий составляют ряд ансамблей нейросетевых моделей класса EfficientNet (патент № 2768797) [9] и метод амплификации и анализа средствами искусственного интеллекта микроизменений в цветах объектов на кадрах (патент № 2774624) [10]. Объединенные в одну систему, они

позволяют с высокой точностью определить синтетически измененные изображения лиц на видео.

Отличительной особенностью системы является возможность обработки видеоконтента с несколькими лицами в кадре. В этом случае система выявляет отдельное лицо, созданное синтетическим образом, и оценивает его достоверность, что позволяет противодействовать ряду методов обхода систем выявления дипфейков.

Разработанные технологии предназначены для использования при решении следующих задач:

− защита от кибератак с обходом систем Face Recognition и Liveness Detection;

− выявление на ранних стадиях информационных атак с целью борьбы с фейковыми новостями;

− обеспечение защиты переговоров по видео-конференц-связи;

− обеспечение защиты от мошеннических действий.

Показатели эффективности системы при замерах на независимых тестовых выборках составили 98 %, что существенно выше показателей опубликованных аналогов.

Важность исследуемой проблемы подтверждается тем, что депутаты выступили с законодательной инициативой о введении ответственности за несанкционированное использование голоса и изображений человека в целях мошенничества.

Таким образом, считаем необходимым разрабатывать методику расследования преступлений, совершенных с использованием искусственного интеллекта, в целях повышения эффективности их расследования.

Список основных источников

1. Ежемесячный сборник о состоянии преступности в России [Электронный ресурс] // Генеральная прокуратура Российской Федерации. Портал правовой статистики. URL: http://crimestat.ru/analytics (дата обращения: 12.01.2024). Перейти к источнику Вернуться к статье

2. Статистические сведения МВД о состоянии преступности за 2023 год // Официальный сайт МВД Российской Федерации. URL: https://xn--b1aew.xn--p1ai/news/item/ (дата обращения: 30.01.2024). Перейти к источнику Вернуться к статье

3. Дипфейк // Большая российская энциклопедия. URL: https://bigenc.ru/c/dipfeik-f9f89b (дата обращения: 03.03.2024). Вернуться к статье

4. Поляков В. В. Источники и принципы формирования частной методики расследования высокотехнологичных преступлений // Lex russica (Русский закон). 2022. 75 (6). С. 85–96. Вернуться к статье

5. Бессонов А. А. О некоторых возможностях современной криминалистики в работе с электронными следами // Вестн. Ун-та им. О. Е. Кутафина (МГЮА). 2019. № 3 (55). С. 46–52. Вернуться к статье

6. Вехов В. Б., Пастухов П. С. Формирование стратегий расследования преступлений на основе положений электронной криминалистики // Ex jure. 2019. № 4. С. 129–141. Вернуться к статье

7. Ищенко Е. П. У истоков цифровой криминалистики // Вестн. Ун-та им. О. Е. Кутафина (МГЮА). 2019. № 3 (55). С. 15–28. Вернуться к статье

8. Россинская Е. Р. К вопросу об инновационном развитии криминалистической науки в эпоху цифровизации // Юрид. вестн. Самарского ун-та. 2019. № 4. С. 144–151. Вернуться к статье

9. Способ и система для определения синтетически измененных изображений лиц на видео [Электронный ресурс] : пат. RU 2768797 / К. Е. Вышегородцев, А. В. Балашов, Г. А. Вельможин, В. В. Сысоев. Опубл. 24.03.2022. URL: https://www1.fips.ru/registers-doc-view/fips_servlet?DB=RUPAT&DocNumber=2768797&TypeFile=html (дата обращения: 30.01.2024). Перейти к источнику Вернуться к статье

10. Способ и система определения синтетических изменений лиц в видео [Электронный ресурс] : пат. RU 2774624 / И. А. Оболенский, В. В. Сысоев, А. В. Балашов. Опубл. 21.06.2022. URL: https://www1.fips.ru/registers-doc-view/fips_servlet?DB=RUPAT&DocNumber=2774624&TypeFile=html (дата обращения: 30.01.2024). Перейти к источнику Вернуться к статье